

Remarks/Arguments

Claims 1-4 and 6-17 are pending.

Claims 1-4 and 6-17 stand rejected.

No claims have been amended.

Rejection of claims 1-4, 7-10 and 12-17 under 35 USC 103(a) as being unpatentable over Kudelski (US Pat No 5144663) in view of Schneier, *Applied Cryptography*

Applicants submit that for the reasons discussed below claim 1 is not unpatentable under 35 USC 103(a) over Kudelski in view of Schneier.

The invention of claim 1 resides, in part, in the recognition by the inventors that a user of digital television services may want a mix of services from several different service providers, each of whom requires either the use of a separate set-top box or a separate smart card (specification; page 1, lines 22-30). A user would thus be required to purchase multiple conditional access smart cards and to swap the cards as the user channel surfs (specification; page 1, lines 33-36). The invention as recited in claim 1 overcomes the problem by providing a method for managing access to a restricted transmitted event, the method comprising, inter alia:

receiving encrypted access information associated with said transmitted event from a particular one of a plurality of service providers, said access information being encrypted using a shared public key that is shared among the plurality of service providers . . .

decrypting said access information in a conditional access module using a private key associated with the shared public key”

Thus, the method of claim 1 provides for using a **shared public key** that is shared among the plurality of service providers to encrypt access information, and using a private key associated with the shared public key to decrypt the access information. The claimed method overcomes the problem of requiring the user to purchase multiple conditional access smart cards and swap cards in order to access information received from different ones of the plurality of services providers.

Kudelski teaches a method and apparatus for implementing a pay television system, wherein code words generated by random number generator 26, and information relating to the identification to be transmitted, are used to generate a scrambled signal (col. 3, line 65 - col. 4, line 4). The code word and the information are recovered at the receiver device to descramble the signal.

The Examiner concedes that "Kudelski does not explicitly disclose using a public key system for encryption the access information." (Office Action, page 3). In fact, Kudelski does not disclose, either explicitly or implicitly, using a public key system for encrypting access information. Furthermore, Kudelski neither discloses nor suggests "receiving encrypted access information associated with said transmitted event from a particular **one of a plurality of service providers**, said access information being encrypted using a **shared public key that is shared among the plurality of service providers.**"

The Examiner further states that Kudelski discloses that the encrypted access information may be encrypted using any encryption system, referring to col. 4, lines 54-57 of Kudelski. However, col. 4, lines 54-57 of Kudelski read as follows:

The code for the permutation is transmitted in enciphered form, e.g. according to the system DES but not exclusively, this system DES being practically unbreakable.

This statement is not the equivalent of stating "the encrypted access information may be encrypted using any encryption system."

The Examiner cites Schneier for a disclosure of hybrid cryptosystems in which a symmetric key is distributed securely by encrypting the symmetric key with a public key at the sender and decrypting the symmetric key with the private key at the receiver. The Examiner states that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Kudelski by encrypting the access information using a public key, in order to gain the benefits of a hybrid cryptosystem, namely the speed of symmetric encryption with less risk of the key being exposed. However, since Kudelski teaches:

The code or key of permutation is transmitted in real time so that even if a pirate finds the right combination, this one is only valid for a very short instant of time, e.g. one second.

(col. 4, lines 50-53), there is no motivation in Kudelski to seek an alternative approach which provides a lower risk of the key being exposed.

The Examiner states that "the cited portions of Schneier are silent as to whether a public key would be shared between a plurality of service providers, as in Claim 1, or if each service provider would have its own public key, as in Claim 7." However, neither Kudelski nor the cited portions of Schneier make any reference to a plurality of service providers. Thus, there is no teaching or suggestion in the cited art that discloses the limitation of a plurality of service providers.

The Examiner has taken official notice that it is well known that a smart card as used by Kudelski for storing a key generally has limited storage space. The Examiner states, based on this official notice, that it would have been obvious to one of ordinary skill in the art at the time the invention was made to have a plurality of service providers share a public key, in order to conserve storage space by only requiring the smart card to store one private key corresponding to the one public key.

The official notice is improperly relied upon as the principal basis on which the rejection is based, as this official notice appears to provide the motivation for the proposed change.

Any rejection based on assertions that a fact is well-known or is common knowledge in the art without documentary evidence to support the examiner's conclusion should be judiciously applied. Furthermore, as noted by the court in *Ahlert*, any facts so noticed should be of notorious character and serve only to "fill in the gaps" in an insubstantial manner which might exist in the evidentiary showing made by the examiner to support a particular ground for rejection. It is never appropriate to rely solely on common knowledge in the art without evidentiary support in the record as the principal evidence upon which a rejection was based. See *Zurko*, 258 F.3d at 1386, 59 USPQ2d at 1697; *Ahlert*, 424 F.2d at 1092, 165 USPQ 421.

MPEP 2144.03.E.

The Examiner's proposed official notice appears to state that the storage space on a smart card is so limited in comparison to the storage needs of a key, that the storage of more than one key is impractical.

For example, assertions of technical facts in the areas of esoteric technology or specific knowledge of the prior art must always be supported by citation to some reference work recognized as standard in the pertinent art.

MPEP 2144.03A. As the Examiner makes an assertion of the size of the storage space on a smart card, and the data storage requirements of a key, these assertions must be supported by citation to some reference work. Moreover, it is respectfully submitted that the storage space on a smart card was more than adequate to store numerous private keys at the time the invention was made. In an example in the specification, the record in the smart card included two 768-bit fields for storing the private key for decrypting the AIMS and for storing the public key for verifying the signature on certificates (page 9, lines 6-7). It is submitted that the storage capacity of a smart card at the time the invention was made was far more than adequate for storing numerous pairs of 768-bit fields for storing pairs of private and public keys.

Moreover, the assertion of official notice with respect to claim 1 is directly contradictory to the assertion of official notice with respect to claim 7. As noted, the official notice with respect to claim 1 states that it is well known that a smart card generally has limited storage space, and that storage space would be conserved by having only one public key/private key pair. The official notice with respect to claim 7 states that it would have been obvious to assign a different respective public key/private key pair to each service provider. Thus, one official notice states that storage space is limited, so that only one private key should be stored, while the other official notice states that it is obvious to store multiple private keys. Thus, the official notice as to claim 1 and the official notice as to claim 7 are mutually inconsistent, and accordingly, such official notice must be withdrawn at least for the sake of consistency, in addition to all of the other reasons set forth in this response.

To adequately traverse such a finding, an applicant must specifically point out the supposed errors in the examiner's action, which would include stating why the noticed fact is not considered to be common knowledge or well-known in the art. See 37 CFR

1.111(b). See also *Chevenard*, 139 F.2d at 713, 60 USPQ at 241 ("[I]n the absence of any demand by appellant for the examiner to produce authority for his statement, we will not consider this contention."). A general allegation that the claims define a patentable invention without any reference to the examiner's assertion of official notice would be inadequate. If applicant adequately traverses the examiner's assertion of official notice, the examiner must provide documentary evidence in the next Office action if the rejection is to be maintained. See 37 CFR 1.104(c)(2). See also *Zurko*, 258 F.3d at 1386, 59 USPQ2d at 1697 ("[T]he Board [or examiner] must point to some concrete evidence in the record in support of these findings" to satisfy the substantial evidence test).

MPEP 2144.03.C.

Since the Examiner's assertion of official notice has been adequately traversed, the Examiner must provide documentary evidence in the next Office Action if this rejection is to be maintained.

Moreover, even assuming *arguendo* the Examiner's assertion of official notice is correct, the asserted motivation would still be lacking. There is nothing in the Examiner's assertion of official notice that supports the desirability of using a single private key to receive transmissions from a plurality of service providers. Rather, as noted above, part of the invention of claim 1 is the recognition of the desirability of using a single smart card to access content from several different service providers. Thus, there is no suggestion or teaching in the prior art to modify the references as proposed by the Examiner.

For at least the foregoing reasons, claim 1 is allowable over the prior art of record.

Claims 2-4 and 15-17 depend from claim 1, and are allowable at least by reason of their dependence on allowable claim 1.

Turning now to independent Claim 7, this claim recites in part:

receiving encrypted access information associated with said transmitted event from a particular one of a plurality of service providers, the encrypted access information from each of said plurality of service providers being encrypted with a respective public key associated with each of said plurality of service providers, said received access information comprising data corresponding to the cost of said transmitted event;

selecting from a plurality of private keys stored in a conditional access module a private key associated with a public key of the particular service provider, and decrypting said received access information in a conditional access module using the selected private key;

Thus, in the embodiment of claim 7, each service provider uses a different public key, and the corresponding private keys are pre-stored in the access device. Again, this embodiment address the problem discussed above regarding access to multiple service providers.

The rejection of claim 7 is similar to the rejection of claim 1, and is traversed for the same reasons, to the extent similar. In addition, as to claim 7, the ~~Examiner takes official notice that "it would have been obvious to one of ordinary skill in the art at the time the invention was made to assign a different respective public key/private key pair to each service provider, in order to minimize the damage done if one private key was compromised. Further, it would have been obvious to select from a plurality of private keys the private key associated with the public key of the particular service provider that was used for encryption and use that selected private key for the decryption."~~ (Office Action, page 4).

The foregoing is also an improper official notice.

In limited circumstances, it is appropriate for an examiner to take official notice of facts not in the record or to rely on "common knowledge" in making a rejection, however such rejections should be judiciously applied.

MPEP 2144.03. Here, the Examiner has sought to take official notice, not of *facts*, but of the *conclusion* of obviousness. Such an assertion of official notice is improper, and thus the rejection of claim 7 must be withdrawn.

As noted above, the official notice with respect to claim 7 is inconsistent with the official notice with respect to claim 1, and thus, at least the official notice as to claim 1 or claim 7 must be withdrawn for this reason.

Furthermore, the Official Action does not identify any teaching or suggestion in the art showing a plurality of service providers. Thus, even if the Examiner's statement "it would have been obvious to one of ordinary skill in the art at the time the invention was made to assign a different respective public key/private key pair

to each service provider, in order to minimize the damage done if one private key was compromised" were not official notice, this statement appears to assess obviousness as compared to a method in which a single public key is shared by a plurality of service providers. In fact, a single public key shared by a plurality of service providers is a limitation of claim 1, which, as demonstrated above, is not taught or suggested in the prior art. The Examiner's rejection is thus nothing more than a rejection of claim 7 as an obvious modification of claim 1. This rejection is entirely improper, and should be withdrawn.

Again, applicants submit that neither Kudelski nor Schneier teach or suggest all limitations of claim 7. As discussed above, both references fail to recognize the problem addressed by the present invention, and fail to mention or suggest any solutions to overcome the problem. Kudelski discloses a system for pay television and Schneier mentions a public key system, but neither discusses or mentions a system for accessing restricted events from multiple service providers. Therefore, applicants submit that claim 7 is patentably distinguishable over Kudelski in view of Schneier.

Claims 8-10 and 12-14 depend from independent claim 7, and are allowable at least by reason of their dependence on an allowable base claim.

Rejection of claims 6 and 11 under 35 USC 103(a) as being unpatentable over Kudelski (US Pat No 5144663) in view of Schneier, *Applied Cryptography*, and further in view of EBU Project Group, "Functional Model of a Conditional Access System"


The EBU Project Group reference is cited as teaching a smart card used in a conditional access system that uses the PCMCIA standard.

Applicants submit that the alleged teachings of the EBU Project Group reference still fail to cure the defect of Kudelski and Schneier as applied to claims 1 and 7, and as such, claims 6 and 11 are patentably distinguishable over the suggested combination of references.

Ser. No. 09/743,653
Internal Docket No. RCA 89131


Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,
Ahmet Mursit Eskicioglu et al.

By: 
Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: 1/26/06

CERTIFICATE OF MAILING	
I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia, 22313-1450 on:	
<u>1-26-06</u> Date	 _____